Navy Laptops Missing from Recruiting Station

(Washington) – Two laptops used for recruiting were stolen from New Jersey Navy Recruiting Station offices in Trenton and Jersey City recently, and local police have turned over investigation of the matter to Navy Criminal Investigative Service. These laptops and several programs on them were password protected on multiple levels and the likelihood of unauthorized access to the personal data is extremely low; however, the Navy is reviewing the data contained in the computers, including personal information on approximately 31,000 individuals (such as recruiters, prospects from school lists and applicants). Approximately 4,000 individuals had social security numbers on the computer. The Navy is in the process of notifying those affected.

Individuals who believe they may be impacted can call the Navy Personnel Command call center in Millington, TN to confirm whether their personal information was on one of the computers. The number to call is 1-866 U ASK NPC (1-866-827-5672).

The Trenton laptop was reported stolen from the recruiting station in early June, and the recruiting stations reported the theft to the police and local authorities. While conducting a command-wide review of Privacy Act data policies and procedures, the information on the theft was provided to the Chief of Naval Personnel in mid July. Initial reports indicate that two categories of information were included on the laptop, either on databases or other documents – a list of applicants and recruiters, as well as information from selective service and school lists.

The Jersey City laptop had the same type of information and databases. It was reported missing in early July and also reported to the Chief of Naval Personnel in mid July.

While police and NCIS investigated the theft, the Navy Recruiting Command conducted a comprehensive accounting and has accounted for all other laptops and computers.

The Navy is taking a number of measures to better ensure personal information security. In the near term, the Navy sent a message to its commands to comprehensively review all procedures to better ensure personal information is safeguarded. Commands are also required to disclose any unauthorized disclosure. These actions are to be completed by Aug. 18.

The Navy will contact individuals on the lists by letter and provided information on how to guard against identity theft. Information on how to watch for suspicious activity on personal accounts is also posted on the NPC web site – www.npc.navy.mil.

There is no evidence that any of the data has been used illegally. However, individuals are encouraged to carefully monitor their bank accounts, credit card accounts and other financial transactions.

Tips on how to watch for suspicious activity:

1. Closely monitor your bank and credit card statements for fraudulent transactions. Monitoring accounts online is the best way to detect fraud early.

2. Place a 90-day fraud alert on your credit report, which tells creditors to contact you before opening any new accounts or making any changes to your existing accounts. This action may cause some delays if you're trying to obtain new credit.

- You only need to contact one of the three companies — Equifax, Experian, or TransUnion — to place an alert. The company you call is required to contact the other two.

- Once you create the fraud alert, you're entitled to free copies of your credit reports. Review these reports for inquiries from companies you haven't contacted or accounts you didn't open.

- If you still want the alert after 90 days, you'll need to renew it.

If you find fraudulent accounts or transactions

1. Contact the financial institution to close the fraudulent accounts or accounts that have been tampered with.

2. File a report with your local police department.

3. File a complaint with the FTC.

- Additional information is located on the NKO website: Course Title - Identity Theft and Catalog Code -FS0406_ENG. Log into NKO, click Learning Tab, click E-learning Auto-Logon Gear link, click advanced search, under course title enter Identity Theft, enroll and begin training.

- The NPC call center in Millington will be manned for Sailors to call and see if their personal data was on the list. The number is 1-866 U ASK NPC. (1-866-827-5672)